July 2019

Internal Control Management by Design

An Integrated & Continuous Approach to Managing Controls

STRATEGY***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Internal Control Management by Design

An Integrated & Continuous Approach to Managing Controls

Monitoring and Managing Controls Effectively

Challenge to Boards, Executives, and GRC Professionals

Organizations fail to monitor and manage controls effectively in an environment that demands agility. Too often internal control management is a periodic exercise that provides incomplete visibility into the organization's people, processes, and systems. This results in inevitable failure of governance, risk management, and compliance that provides case studies for future generations on how poor internal control management leads to the demise of organizations: even those with strong brands.

Gone are the years of simplicity in business operations. Exponential growth and change in risks, regulations, globalization, employees, distributed operations, competitive velocity, technology, and business data encumbers organizations of all sizes. Keeping this risk, complexity, and change in sync is a significant challenge for boards, executives, as well as GRC management professionals throughout all levels of the business. This challenge is even greater when internal control management is not an ongoing and monitored process in the organization that is connected to and enables all aspects of GRC. Organizations need to understand how to design effective controls, implement them, and review whether the risks they were designed to control are effectively mitigated on a continuous and ongoing basis.

Corporate governance and organizational culture have largely been based on trust. In this context the organization trusts their employees, contractors, and other third parties working on its behalf. It is understood that these individuals will read and remember policies and procedures, hold themselves accountable to them, and apply those policies and procedures in their daily activities. The reality is that people are human. They make mistakes, they cut corners, and their own motives and goals may not align with the organizations. This is further confounded when management undermines controls they find are bothersome. Keeping up with controls in a changing workforce environment as regulations, risks, applications, priorities, and business processes change is challenging. There is a greater need to define and automate the breadth of internal controls to bring real-time insight into what individuals are actually doing across the enterprise, in order to mitigate user access and process risks.

Internal control management in the modern organization is:

- **Distributed.** Even the smallest of organizations can have distributed operations complicated by a web of interrelated transactions, processes, and relationships.

The traditional brick and mortar business with physical buildings and conventional employees has been replaced with an interconnected mesh of relationships and interactions which define the organization. Complexity grows as these interconnected roles, relationships, and processes move to an increasing number of systems.

- **Dynamic.** Organizations are in a constant state of change as distributed operations and systems grow and evolve. At the same time, the organization is trying to remain competitive with shifting employees, business strategies, technologies, partners, and processes while also keeping pace with change to risk environments that impact internal controls. The multiplicity of environments that organizations have to monitor span regulatory, geopolitical, market, credit, and operational risks. Managing internal controls and business change on numerous fronts has buried many organizations.

- **Disrupted.** The explosion of data in organizations has brought on the era of "Big Data." Organizations are attempting to manage high volumes of structured and unstructured data across multiple systems, transactions, processes, roles, and relationships to see the big picture of risk and controls. The velocity, variety, veracity, and volume of control data is overwhelming – disrupting the organization and slowing it down at a time when it needs to be agile and fast.

- **Accountable.** There is growing awareness among executives and directors that internal control management needs to be taken seriously. It is part of their fiduciary obligations to oversee controls, and their intersection with risk and compliance, as an integrated part of business strategy and execution. Furthermore, regulations that are increasing personal liability within these roles put an emphasis on business leaders taking greater interest and accountability for risk, control, and compliance.

Understanding the Interrelationship of Controls and Their Impact

Internal control management is often misunderstood, misapplied, and misinterpreted as a result of scattered and uncoordinated approaches that get in the way of sharing data. This is particularly true when internal control management is a set of manual processes encumbered by documents, spreadsheets, and emails when it could be continuously monitored and enforced. Internal controls are pervasive; there are a variety of departments that manage controls with varying approaches, models, needs, and views on what controls are and how they should be measured and managed. These challenges come at department and process levels, and continue to build as organizations develop broader GRC and enterprise/operational risk management strategies that span these departments.

The management of internal controls has become increasingly challenging as the organization has:

- *Multiple lines of business* operating globally across many jurisdictions and systems.

- *Workforce that is constantly changing* with access into systems and processes. Over time there are significant gaps and rights issues as the average user has access into a dozen systems or more.

- *Web of third party relationships* of contractors, consultants, temporary workers, service providers and outsourcers that have access to data, systems, and processes.

- *Mergers and acquisitions that exponentially grows* the systems, processes, and controls in the organization if not properly integrated.

- *Isolated systems that monitor controls from a myopic perspective* but fail to see the issues and rights across systems in a heterogenous environment.

- *Migration of applications to the Cloud* without IT involvement that provides further challenges to monitoring controls.

- *Millions of dollars in transactions* that flow through business systems in the digital economy that need controls.

For some organizations, internal control management is only a view of routine financial controls, resulting in nothing more than a deeper look into siloed ERP systems, and does not truly provide an enterprise view of controls across roles, business systems, processes, and operations. Completing a control assessment process and ticking the box has got in the way of true control analysis and understanding.

GRC is a "capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]."[1] Internal controls are a critical foundation to all three aspects of GRC. Controls aid the organization in reliably achieving objectives, controls manage uncertainty by mitigating risk, and controls are a critical part of meeting compliance obligations and enabling the organization to act with integrity. Good internal controls result in predicable business behavior, transactions, access, and processes.

Internal control silos — where distributed systems and processes maintain their own controls, data, analytics — pose a major challenge to achieving this. Documents and spreadsheets are not equipped to capture the complex interrelationships that span systems, operations, transactions, lines of business, and processes. Individual business applications focus on their view of controls and not the aggregate picture, unable to recognize substantial and preventable losses. When an organization approaches internal controls in scattered silos without acknowledging interrelationships across silos, there is little opportunity to be intelligent about risk and control. This is due to the fact that processes intersect, compound, and interrelate to create a larger risk exposure than each silo is independently aware of. A siloed approach to internal controls fails to deliver insight and context, and renders making a connection between controls and risk management, objectives, and performance nearly impossible. Control accountability is frequently distributed across different board level owners. Today it is critical that these

1 *This is the official definition of GRC as published in the GRC Capability Model at www.OCEG.org.*

roles are all working off the same data and that this control data is clean, reliable, and timely.

Making sense of internal control management and its varying factions across operational, financial, employee conduct, regulatory, and IT risks can be bewildering. An internal control management strategy that is siloed and myopic makes enterprise and operational risk management a challenge. This is exponentially compounded when risk velocity is considered: when risk materializes into an event it moves very quickly and controls are missing. Are organizations agile enough to react?

Providing 360° Contextual Awareness of Controls

The physicist, Fritjof Capra, made an insightful observation on living organisms and ecosystems that also rings true when applied to internal control management:

"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."
Fritjof Capra

Capra's point is that biological ecosystems are complex, interconnected, and require a holistic understanding of the intricacy in interrelationships as an integrated whole, rather than a dissociated collection of parts. Change in one segment of an ecosystem has cascading effects and impacts to the entire ecosystem.

"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."
Fritjof Capra

This is true in internal control management. What complicates this is the exponential effect of risk and control on the organization. Business operates in a world of chaos. Applying chaos theory to business is like the 'butterfly effect' in which the simple flutter of a butterfly's wings creates tiny changes in the atmosphere that could ultimately impact the development and path of a hurricane. A small event cascades, develops, and influences what ends up being a significant issue. Dissociated siloed approaches to internal controls that do not span data, systems, employee and third party access/roles, and processes can leave the organization with fragments of truth that fail to see the big picture of risk and controls across the enterprise, as well as how it supports their strategy and objectives. The organization has to have holistic visibility and 360° contextual awareness into control and risk relationships across the enterprise. Complexity of business and intricacy, and interconnectedness of control data, requires that the organization implement an enterprise view of internal controls as part of a broader GRC/ERM strategy.

Technology for internal control management, automation, and continuous monitoring now enable organizations to achieve a real-time, integrated view of enterprise risks and controls across business systems, applications, processes, and roles. This not only enables an enterprise perspective of GRC, but also allows the organization to increase

efficiency, effectiveness, and agility in internal control management.

Managing internal controls effectively requires integration across business systems and processes. This delivers 360° contextual awareness and analysis of controls that enables an organization with a full perspective of controls and access across systems and processes.

Managing internal controls effectively requires integration across business systems and processes. This delivers 360° contextual awareness and analysis of controls that enables an organization with a full perspective of controls and access across systems and processes. Next generation internal control management is built on an integration of controls and management process, information, and technology architecture that can show the relationship between objectives, access, roles, risks, controls, and events. The demand is for predictive analytics to extract from this mass amount of data and automate the management and monitoring of controls to prevent losses, events, and incidents, and further help strategic business, department, and operational objectives succeed.

This is enabled through a federated and connected view of internal controls that leverages artificial intelligence, machine learning, and integrated process automation to make the internal control management process more efficient, effective, and agile. This in turn enables organizations to spend more time focusing on the analysis of risk in the context of the organization, its strategy, objectives, and the users conducting business and less on manually assessing the state of controls as it is now automated. Technology makes it easier to share data, while still maintaining independence of thought and action across the organization.

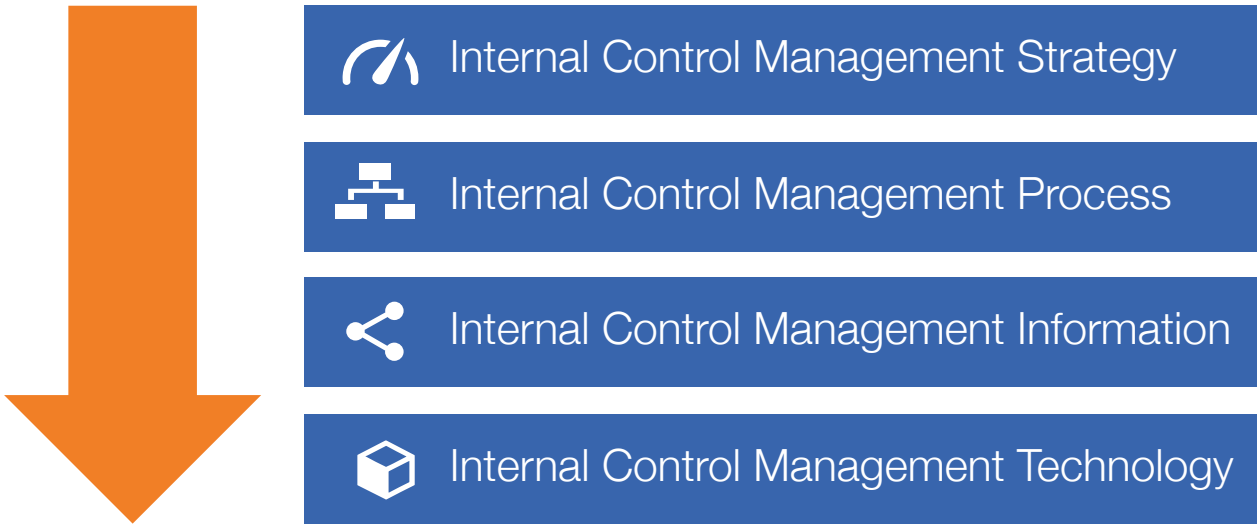
The bottom line: Organizations are best served to take an enterprise and automated approach to internal control management across employee and third party access, business systems, and processes. This can then roll into enterprise and operational risk management and reporting that supports business objectives and is integrated with decision-making processes. This can be done through a common internal control management strategy, process, and technology architecture that supports overall internal control management activities and automated continuous enforcement from the user and process level up through an enterprise view.

Internal Control Management by Design

Different Approaches Organizations Take in Managing Controls

The primary directive of a mature internal control management program is to deliver effectiveness, efficiency, and agility to business operations and processes. This is in the context of managing the breadth of controls across organizational systems, processes, and users. This requires a strategy that connects the enterprise systems, business units, processes, users, transactions, and information to enable transparency, discipline, and control of the ecosystem of controls across the enterprise.

Internal Control Management: a Top Down Approach



GRC 20/20 has identified three approaches organizations can take to better manage risk:

- **Anarchy – ad hoc manual approaches to controls.** This is when the organization has varying manual processes encumbered by documents, spreadsheets, and emails to manage and monitor controls. Manual and siloed internal control management initiatives never see the big picture and fail to put control management in the context of organization objectives, user activities, and risk management. The organization is not thinking big picture about how internal control management and automation can be designed to meet a range of needs across systems, processes, and users. An ad hoc approach to internal control management results in poor visibility into the organization's systems, as there is no integration for bringing the big picture together; there is no possibility to be insightful about controls and risk. The organization fails to see the web of control interconnectedness and its impact on performance and strategy, leading to greater exposure than any silo understood on its own.

- **Monarchies of isolated controls – myopic view.** If the anarchy approach does not work then the natural reaction is centralization of controls in departments, processes, and applications. However, this has its issues as well. Organizations become susceptible to one view of controls that are very focused in one system or process without perhaps fully understanding the breadth and scope of controls and their interrelationships across business systems and processes. From a technology point of view, it may force many parts of the organization into managing a limited scope of controls, and watering down risk management.

- **Federated – an integrated and automated enterprise approach.** The federated approach is where mature organizations will find the greatest balance in a collaborative and integrated view of control management and automation

across access, roles and responsibilities, business systems and processes. It allows for some level of process and business function autonomy when needed, but also focuses on a common technology architecture that the various groups across internal control management participate in. A federated approach on an integrated control management platform increases the ability to connect, understand, analyze, and monitor connectedness and underlying patterns of controls across business systems, processes, users, and risk relationships. Mainly as it allows different business functions to be focused on their areas while reporting into a common control architecture and monitoring/automation framework. Different functions participate in control management, with a focus on coordination and collaboration through a common core architecture that integrates across business systems, processes, and users.

Organizations that continue to conduct manual, periodic assessments will increasingly position themselves at a competitive disadvantage to those that can automate the management and continuous enforcement of controls in their environment. Control automation across business systems, processes, and users is needed to address:

- Ever-changing business environment, where critical risks are more likely to be missed in manual or siloed processes
- Ineffective reactive approach that tends to identify control issues after they've become a problem
- Efficiencies to reduce costly resources that can't scale to continuously cover all controls
- Incomplete information upon which to make decisions

An enterprise view, and automation of controls, enables an organization with a real-time, integrated view of enterprise risk and performance to proactively automate and address emerging risks in systems and processes as they happen. It also enables the organization to reduce the cost of compliance by eliminating the need to manually collect, aggregate, analyze, and report on controls. Efficiency is gained through fewer sample tests, fewer control tests, fewer mitigating controls, while providing 100% control testing and enforcement that is automated. The organization saves time and resources managing risk by exception and saves internal and external audit costs, as they no longer need to manually re-perform audit activities on controls that have been automated.

Internal Control Management Architecture

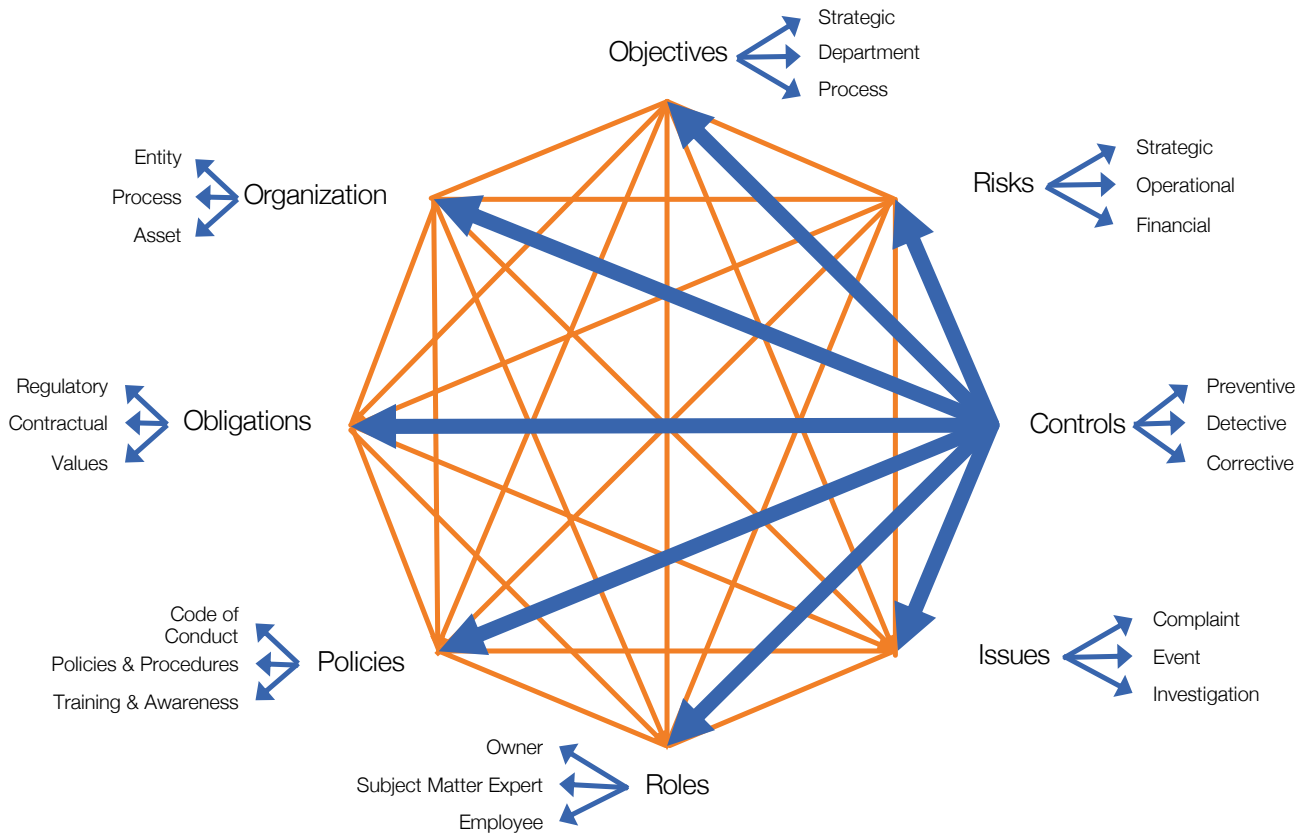
An internal control management strategy is supported and operationalized through an internal control management architecture. Organizations require complete situational and holistic awareness of controls across access, operations, processes, systems, users, roles/responsibilities, transactions, and data to see the big picture in the context of organizational operations. Distributed, dynamic, and disrupted business requires the organization to take a strategic approach to internal control management architecture. The architecture defines how organizational processes, information, and technology is

structured to make internal control management effective, efficient, and agile across the organization and the application users conducting business.

Internal control management fails when information is scattered, redundant, non-reliable, and managed as a system of parts that do not integrate and work as an automated collective whole. The internal control management architecture supports internal control processes and overall GRC and risk management strategy. With processes defined and structured, the organization can now define the architecture needed to support internal control management and automation across systems.

A successful internal control automation architecture will be able to connect information across risk management and business systems. This requires a robust and adaptable control architecture that can model the complexity of risk information, user entitlements, transactions, interactions, relationship, cause and effect, and the analysis of information - which can integrate and manage a range of business systems and associated controls. The right technology architecture enables the organization to effectively manage and automate controls, and facilitate the ability to document, communicate, report, and monitor a range of assessments, documents, tasks, responsibilities, and action plans.

There can and should be a central core technology platform for control management that connects the fabric of the control processes, information, and other technologies together across the organization. But this is the hub of control management and requires that it be able to integrate and connect with a variety of other business systems.



Many organizations see initiatives fail when they purchase technology before understanding the breadth of their process, and information architecture requirements. The right internal control management and automation technology choice for an organization facilitates the integration and correlation of control information, analytics, and reporting. Organizations suffer when they take a myopic view of control management technology that fails to connect all the dots and provide context to business analytics, performance, objectives, and strategy in the real-time that a business operates in.

Internal control automation technology has evolved. GRC 20/20 has monitored this over the years as we have seen progression that brings technologies into a new generation of solutions. These solutions allow for greater user experience, while providing connectivity and integration across business systems to automate and manage interconnected risk, access, and control relationships. They have advanced analytical capabilities and are beginning to leverage artificial intelligence and cognitive computing with predictive analytics, machine learning, and natural language processing.

The performance and usability of the new generation of internal control management and automation in the context of GRC technology returns value to the organization through efficiency, effectiveness, and agility - providing strong overall performance of the solution, and the agility and rapid implementation timeframes through a low-code configurable solution.

Some of the core capabilities organizations should consider in their internal controls automation and management platform are:

- **Integration.** Internal control management is not a single isolated competency or technology within a company. It needs to integrate across business systems, processes, and users. Understanding and controlling what users can and should be doing is essential to an effective internal control program. Systems that simply integrate data without providing user context – who they are, their role, what they can do and what they are actually doing in relation to controls and company objectives – put the program at a significant disadvantage when responding to risk. The ability to pull and push data through integration is also critical. Systems that pull data can only react to events after they occur. Systems that pull and push data in real-time, however, can prevent the event from occurring.

- **360° contextual awareness.** The organization should have a complete view of what is happening with controls in the context of risk and compliance. Contextual awareness requires that control management have a central nervous system to capture signals found in business systems, user accounts, processes, data, and transactions so the organization knows who, what, where, and how - while quickly and effectively remediate risk and improve performance. It also needs to capture changing business and risks for interpretation, analysis, and holistic awareness of controls in the context of risk and compliance.

- **Support for multiple control initiatives.** The control management and automation technology should allow the organization to harmonize control management across the enterprise. The business can use different business

systems in various parts of the organization and still integrate control data and reporting with an enterprise perspective.

- **Define and map objectives and controls to risk.** Controls are used to mitigate and monitor risk. Every control in the environment maps to the risks addressed, using an integrated risk and control framework. Risk technology should allow for the complete integration and reporting on objectives and controls in the context of their relationship to risk across the enterprise.

- **Allocate control accountability.** Internal control management requires that someone is responsible for controls, and the right technology tracks control ownership and steps taken to maintain compliance through a control taxonomy - enforcing accountability through task management, workflow, and escalation. Through reporting and metrics, control owners see risk from different perspectives and understand what they are responsible for. In order for someone to accept responsibility for risk, their ability to understand the risk is critical. Simply telling someone something is high risk is not as effective at establishing accountability as letting them know the potential impact of the risk.

- **Advanced control reporting and trending.** Internal control technology manages and monitors risk at the enterprise level, and should provide visibility into risks across businesses, departments, and, ideally, all the way down to specific users and their transaction details. This permits detailed reporting, dashboards, trending, and analytics that scale to the needs of the department or enterprise. Organizations can establish and monitor control metrics and map them to objectives and processes. Reporting is customizable and scalable to the context and level of detail appropriate to the audience — whether it be process owners, managers, executives, or board members.

- **Control analytics and modeling.** Mature internal control automation technology should support a breadth of control analytics and modeling to meet the diverse needs of groups across the business. The solution can track and model spending to treat controls in the context of risk exposure.

- **Understand the interrelationship of controls and risk.** Internal control management and automation technology provides for identification and categorization of controls into structures to effectively manage and assign accountability. However, individual controls can also relate to risk outside of a hierarchical model. The control information architecture allows for the categorization and mapping of controls to risks, objectives, regulations, standards, frameworks, and organizational structures.

GRC 20/20's Final Perspective

To maintain the integrity of the organization and execute on strategy, the organization has to be able to see the individual control (the tree), as well as the interconnectedness of controls and risk (the forest). Many organizations are asking for this to go even deeper,

as they need to see the leaf and branch as it connects to the tree and how it is part of the forest.

Internal control and risk management in business is non-linear. It is not a simple equation of 1 + 1 = 2. It is a mesh of exponential, and a sometimes chaotic, relationship and impact in which 1 + 1 = 3, 30, or 300. What seems like a small control issue or exposure may have a massive effect or no effect at all. In a linear system, effect is proportional with cause, in the non-linear world of business, risks without controls are exponential. Business is chaos theory realized. The small flutter of control exposure can bring down the organization. If we fail to see the interconnections of controls and risk on the non-linear world of business, the result is often exponential to unpredictable.

Internal control management and automation enables the organization to understand and automate controls in the context of risk. It can weigh multiple inputs from business systems, processes and users, and use a variety of methods to analyze controls and provide qualitative and quantitative risk modeling.

Successful internal control management requires the organization to provide an integrated user, process, information, and technology architecture for control automation. This helps to identify, analyze, manage, and monitor controls, and capture changes in the organization's risk profile. Mature internal control management is a seamless part of governance and operations. It requires the organization to take a top-down view of controls in context of risk, led by the executives and the board, and make up part of the fabric of the business, not an unattached layer of oversight. It also involves bottom-up participation where business functions at all levels identify and monitor controls and the impact of risk.

Organizations striving to increase internal control management maturity in their organization become more:

- **Aware.** They want to have a finger on the pulse of the business and watch for change in the business environments that introduce risk and need controls. Key to this is the ability to turn data into information that can be, and is, analyzed and shareable in every relevant direction.

- **Aligned.** They need to align control and risk management to support and inform business objectives across systems, processes, and users. This requires continuously aligning objectives and operations of the integrated and automated control capability to the objectives and operations of the entity, and to give strategic consideration to information from the control management capability to affect appropriate change.

- **Responsive.** Organizations cannot react to something they do not sense. Internal control automation is focused on gaining greater awareness and understanding of information across business systems, users, and transactions – helping to improve transparency, but also quickly cutting through the morass of data to what an organization needs to make the right decisions.

- **Agile.** Stakeholders desire the control automation to be more than fast; they require it to be nimble. Being fast isn't helpful if the organization systems, processes, people, and transactions are out of control and headed in the wrong direction. Control automation enables decisions and actions that are quick, coordinated, and well thought out. Agility allows an entity to use controls to its advantage and be confident in its ability to stay on course.

- **Resilient.** The best laid plans of mice and men fail. Organizations need to be able to bounce back quickly from changes in context and risks with limited business impact. They desire to have sufficient control tolerances to allow for some missteps and have the confidence necessary to rapidly adapt and respond to opportunities.

- **Efficient.** They want to build business muscle and trim fat to rid expense from unnecessary control overhead, duplication, redundancy, and misallocation of resources; to make the organization leaner overall with enhanced capability and automation across business applications and processes.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com